ORIGINAL

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* A residence located at 903 Hershey Avenue in Monterey Park, California, as described in Attachment A	)	Case No. 2:19-mj-113

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for____days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 1-15-19 3:55 pm

Judge's signature

City and state: Los Angeles, CA

Printed name and title

SAUSA: S. Fernandez x3152

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
2:19-MJ-113	1/17/2019 0600	ASHLEY GARCIA VARELAS

Inventory made in the presence of :

SA VICTOR DOMINGUEZ & SA PATRICIC LEWIS

Inventory of the property taken and name of any person(s) seized:

MISCELLANEOUS DOCUMENTS FROM GARAGE

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 1/24/19

Executing officer's signature

NELSON HERMOSILLO, SPECIAL AGENT

Printed name and title

ATTACHMENT A

PREMISES TO BE SEARCHED

The SUBJECT PREMISES is a two-story house with an orange stucco exterior, dark trim, and a tile roof. It is surrounded by a fence that is partially metal and partially cinderblock. To the rear of the house is a detached garage of the same color as the main house. It is located at 903 Hershey Avenue Monterey Park, CA 91755. The SUBJECT PREMISES is located near the intersection of Hershey Avenue and New Avenue.

The area to be searched includes all rooms, annexes, attics, basements, porches, garages, carports, outside yard, curtilage, mailboxes, trash containers, debris boxes, storage lockers, locked containers and safes, cabinets, rooms, outbuildings, sheds and outbuildings associated with this

subject premise and shall extend into desks, cabinets, safes, briefcases, backpacks, wallets, purses, trash receptacles, electronic storage devices, any vehicles or boats parked on the property or in the driveway specifically associated with, or assigned to the SUBJECT PREMISES.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of violations of 18 U.S.C. §§ 1546: Fraud and Misuse of Visas, Permits, and Other Documents; 1028: Fraud and Related Activity in Connection with Identification Documents, Authentication Features and Information; 2342(a), 2344(a): Trafficking in Contraband Cigarettes ("the Subject Offenses"), namely:

a. Counterfeit, forged or altered documents to include, but not limited to i-551 Legal Permanent Resident Cards, Social Security Cards, Passports, State Driver's Licenses, Employment Authorization Cards and similar items.

b. Equipment and tools used to facilitate the production of counterfeit, forged or altered documents to include, but not limited to, printing equipment, lamination equipment and graphic arts tools, software and personal computing devices.

c. Cigarettes that are not authorized for sale in the United States; an Officer with the U.S. Customs and Border Protection will be present at the time of the search to determine whether any cigarettes found are authorized for sale in the United States.

d. Any documents, records, identity documents, or debit or credit cards, containing the personal identifying information of any individuals other than Jiali LIANG ("LIANG") and/or other residents of the SUBJECT PREMISES.

e. Financial and business records relating to the sale of cigarettes and counterfeit documents, as well as personal financial records for LIANG, in paper and/or electronic form, for the period of 2017 to the present, including the following:

i. Income statements; cash flow statements; profit and loss statements; balance sheets; general ledgers, chart of accounts, and any work papers used in the course of preparing and/or maintaining the books and records relating to the sale of cigarettes and counterfeit documents;

ii. Invoices and records of expenditures relating to the sale of cigarettes and counterfeit documents;

iii. Shipment records and packaging supplies;

iv. Bank statements, check registers, cancelled checks, deposit and withdrawal items, credit card receipts and statements, financial instruments, wire transfers, invoices, general ledgers, and receipt books.

f. Materials for use in the production of counterfeit documents including design software, paper stock, ink, seals, and printing equipment.

g. Hard copies or electronic telephone books and address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, documents and other items or ~~less~~ reflecting names, addresses, telephone numbers, addresses and communications among and between members and associates relating to the above-listed offenses.

h. Records of off-site locations to store records, including safe deposit box keys, records and receipts and rental agreements for storage facilities.

i. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

2. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the attachment of other devices;

d. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. Evidence of the times the device was used;

f. Passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

g. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. Records of or information about Internet Protocol addresses used by the device;

i. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

j. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, WeChat, and WhatsApp Messenger), SMS text, email communications or other text or written communications sent to or received from any digital device relating to the sale of cigarettes or counterfeit documents.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

4. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units;

desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

5. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

c. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

d. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

e. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques

f. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

g. If the search determines that a digital device does not contain any data falling within the list of items to be

seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

h. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

i. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

j. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

k. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

h. During the execution of this search warrant, law enforcement is permitted to: (1) depress [~~TARGET~~] Liang's thumb- and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of ~~[TARGET]'s~~ Liang's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in

order to gain access to the contents of any such device. [ALTERNATIVE, WITH ADDITIONAL EXPLANATION IN AFFIDAVIT: During the execution of this search warrant, with respect to any person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that falls within the scope of the warrant, law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of the person onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of the person with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.] In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.